IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No. 8175
Partha Bhattacharya, et al.	Group Art Unit No.: 2431
Serial No.: 10/044,019	Examiner: Aravind K. Moorthy
Filed on: January 11, 2002	

For: METHOD AND APPARATUS FOR COMPARING ACCESS CONTROL LISTS FOR CONFIGURING A SECURITY POLICY ON A NETWORK

Mail Stop Appeal Brief – Patents
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 20231

APPEAL BRIEF

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed on February 26, 2009, and further to the Notice of Panel Decision from Pre-Appeal Brief Review mailed on May 4, 2009.

I. REAL PARTY IN INTEREST

The real party in interest is Cisco Systems, Inc., which wholly owns the assignee Cisco Technology, Inc.

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals or interferences.

III. STATUS OF CLAIMS

Claims 10, 11, 14-16, 33-35 and 37-44 are pending, were finally rejected, and are the subject of this appeal. Claims 1-9, 12, 13, 17-32, 36 and 45-48 have been canceled.

IV. STATUS OF AMENDMENTS

Claim amendments for the sole purpose of canceling Claims 36 and 45-48 are filed

concurrently with this Appeal Brief in a separate paper under C.F.R. § 1.116(b)(1). The Examiner has not reviewed and entered these claim amendments concurrently filed with this Appeal Brief.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present application contains independent claims 33 and 37. All references in this section refer to Appellant's application specification and drawings.

Claim 33

Claim 33 is directed to a method of comparing access control lists to configure a security policy on a network (*see, e.g.*, page 8, lines 24-27; FIG. 5), the method comprising the computer-implemented steps of:

subtracting a particular access control entry from another access control entry, wherein both the particular access control entry and said another control entry are two access control entries of multiple first access control entries and wherein the first access control entries, including the particular access control entry and said another access control entry, are all of access control entries as specified in a first access control list (*see, e.g.*, page 10, line 15 – page 11, line 2; page 18, lines 1 – 6; page 18, line 21 – page 19, line 3; 110 of FIG. 1; 320 of FIG. 3; FIG. 4A);

identifying one or more first sub-entries in the first access control list, wherein the one or more first sub-entries include each of overlapping sections and non-overlapping sections of all of the first access control entries and wherein at least one of the one or more first sub-entries is derived from results of subtracting the particular access control entry from said another access control entry (*see, e.g.*, page 19, lines 4 – 24; page 22, lines 21 – 24; FIG. 4A); and

programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is contained by one or more entries of multiple second access control entries in the second access control list (*see, e.g.*, page 23, line 7 – page 25, line 6; 130 of FIG. 1; FIG. 4B).

Claim 37

Claim 37 is directed to a policy server communicatively coupled to security devices in a network to configure a security policy on a network (*see*, *e.g.*, FIG. 5), the policy server comprising:

a processor (*see*, *e.g.*, 604 of FIG. 6);

a network interface that communicatively couples the processor to the network to receive flows of packets therefrom (*see*, *e.g.*, 618 of FIG. 6);

a memory (*see*, *e.g.*, 606, 608, or 610 of FIG. 6); and

sequences of instructions in the memory which, when executed by the processor, cause the processor to carry out the steps of (*see*, *e.g.*, page 26, lines 10 - 21):

subtracting a particular access control entry from another access control entry, wherein both the particular access control entry and said another control entry are two access control entries of multiple first access control entries and wherein the first access control entries, including the particular access control entry and said another access control entry, are all of access control entries as specified in a first access control list (*see*, *e.g.*, page 10, line 15 – page 11, line 2; page 18, lines 1 – 6; page 18, line 21 – page 19, line 3; 110 of FIG. 1; 320 of FIG. 3; FIG. 4A);

identifying one or more first sub-entries in the first access control list, wherein the one or more first sub-entries include each of overlapping sections and non-overlapping sections of all of the first access control entries and wherein at least one of the one or more first sub-entries is derived from results of subtracting the particular access control entry from said another access control entry (*see*, *e.g.*, page 19, lines 4 – 24; page 22, lines 21 – 24; FIG. 4A); and

programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is contained by one or more entries of multiple second access control entries in the second access control list (*see*, *e.g.*, page 23, line 7 – page 25, line 6; 130 of FIG. 1; FIG. 4B).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 10, 11, 33-41 and 45-48 are rejected under 35 U.S.C. § 102(b) as allegedly anticipated by Caronni et al., U.S. Pat. No. 5,761,669 (hereinafter *Caronni*).

Claims 14 and 42 are rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Carroni* in view of Brawn et al., U.S. Pat. No. 7,020,718 (hereinafter *Brawn*).

Claims 15 and 43 are rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Carroni* in view of Mate et al., U.S. Pat. No. 7,020,098 B2 (hereinafter *Mate*).

Claims 16 and 44 are rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Carroni* in view of Banginwar et al., U.S. Pat. No. 6,611,863 B2 (hereinafter *Banginwar*).

The rejections of Claims 36 and 45-48 are moot as these claims have been canceled in the concurrently filed claim amendments under 37 C.F.R. § 1.116(b)(1).

The rejections of Claims 10, 11, 14-16, 33-35 and 37-44 are the subject of this appeal. The specific questions presented are:

1. Whether Claims 10, 11, 33-35, and 37-41 are properly rejected under 35 U.S.C. § 102(b) as anticipated by Caronni?

2. Whether Claims 14 and 42 are properly rejected under 35 U.S.C. § 103(a) over *Carroni* in view of *Brawn*?

3. Whether Claims 15 and 43 are properly rejected under 35 U.S.C. § 103(a) over *Carroni* in view of *Mate*?

4. Whether Claims 16 and 44 are properly rejected under 35 U.S.C. § 103(a) over *Carroni* in view of *Banginwar*

VII. ARGUMENT

A. *Caronni* Fails to Anticipate Each and Every Limitation of Each of Claims 10, 11, 33-41 and 45-48.

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The

identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The present record fails to present a *prima facie* case of anticipation because the cited references fail to teach, disclose or suggest every feature of the claims that are rejected for anticipation. Therefore, the rejections should be reversed.

Independent Claim 33

Claim 33 recites:

subtracting a particular access control entry from another access control entry, wherein both the particular access control entry and said another control entry are two access control entries of multiple first access control entries and wherein the first access control entries, including the particular access control entry and said another access control entry, are all of access control entries as specified in a first access control list;

identifying one or more first sub-entries in the first access control list, wherein the one or more first sub-entries include each of overlapping sections and non-overlapping sections of all of the first access control entries and wherein at least one of the one or more first sub-entries is derived from results of subtracting the particular access control entry from said another access control entry; and

programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is contained by one or more entries of multiple second access control entries in the second access control list.

In Claim 33, first access control entries are specified in a first access control list (ACL). In contrast, first sub-entries are identified in the first access control list and include each of overlapping sections and non-overlapping sections of all of the first access control entries specified in the first access control list. At least one of the first sub-entries is derived from the results of subtracting a particular access control entry specified in the first access control list from another access control entry specified in the same first access control list. To

programmatically determine whether the first access control list is functionally equivalent to a second access control list, each of the first sub-entries is determined whether it is contained by one or more of multiple second access control entries in the second access control list.

A benefit of this approach is that, by subtracting first entries specified in the first ACL, even if a section that is subject to access control is contained in two or more of these first entries and therefore overlapped by these first entries, such a section can be represented by a single sub-entry only once. Thus, even if the first entries of the ACL are highly redundant or overlapping, it is not necessary to perform repetitive comparison operations between two ACLs using the highly redundant or overlapping first entries directly. Instead, the sub-entries will be used to determine the functional equivalency of the two ACLs.

Caronni describes an apparatus for allowing communications to a target host on a network to be upgraded from a non-secured session to a secure session. *See* Abstract. Each host uses an ACL to track the encryption capabilities of hosts with which the host is currently communicating. *See Id. at* col. 2, lines 51-54. Each ACL is in a different host of *Caronni*; therefore, each ACL is necessarily and by definition distinct from all the others. The ACLs are not compared as recited in the claim.

Caronni fails to disclose determining the functional equivalency of two ACLs, as featured in Claim 33. In *Caronni*, two hosts start an unsecure communication mode in which clear traffic is to be used (col. 4, lines 62-65). The two hosts engage in certificate discovery protocol (CDP) to exchange key information (*Id. at* col. 4, line 66-col. 7, line 31). The two hosts may upgrade the unsecure communication mode to a secure communication mode based on the exchanged key information (*Id. at* col. 7, lines 32-39).

The Examiner cites *Caronni*'s Abstract and col. 7, line 51 to col. 8, line 13 as allegedly disclosing all the features of Claim 33; the Examiner repeats this citation is repeated for **every** claimed feature. However, the Examiner provides **no reasoning** about why the cited excerpts allegedly disclose all the features of Claim 33, and they do not. The Examiner fails to specify which entities of *Caronni* correspond to the first access control list and the second access control

list in Claim 33, which entity of *Caronni* corresponds to the first access control entries in the first access control list, and which entity of *Caronni* corresponds to the sub-entries in the first access control list – and these features are missing from *Caronni*. The failure of the Examiner to identify which entities of *Caronni* correspond to the first access control list and the second access control list of Claim 33 cannot possibly satisfy the requirement of Section 102, and the applicable case law, that the prior art must show each and every element of the rejected claim. For at least this reason, the Examiner fails to state a *prima facie* case of unpatentability.

Moreover, the Abstract and the cited part of column 7-8 clearly fail to disclose the claimed technique. The Abstract describes creating an access control entry in one access control list and then updating the same list. Col. 7, line 51 to col. 8, line 13 states:

> An option should be provided for ACL daemon 4 to add optional encrypted ACL entries with a TTL of 0. This would allow clear sites to upgrade to encrypted communication, but provide for no automatic fall-back. Once a host used encryption, manual removal of the ACL entry would be necessary.
>
> When host 1 receives an encrypted packet from a target host that does not have an entry in ACL 2 (assuming an optional encryption default case)--perhaps due to the ACL entry for the target host in ACL 2 being expired--if host 1 has received an NSID 13 encrypted packet, ACL daemon 4 should complete an NSID 13 CDP GET/PUT with the target host again, and add the optional encryption ACL entry to ACL 2.
>
> As mentioned above, in the preferred embodiment, the default value for TTL's should be on the order of 5 minutes, since TTL expiration is used to help clear ACL 2 of the hosts which have lost their ability to speak SKIP, but for which host 1 has not an ICMP.sub.-- PROTOCOL.sub.-- UNREACHABLE message. Using an overly large value for the default TTL would prevent host 1 from speaking with a host that lost its ability to speak SKIP for an undue long period of time--i.e., the amount of time of the overly large default TTL value. However, setting the default TTL to a very small value can cause premature removal of entries from ACL 2 in situations, for example, where network latency

or other delays prevents communications from a particular host from reaching host 1 in a time before the TTL for that host reaches zero.

Nothing in this portion discusses determining functionally equivalency of two ACLs, much less determining whether sub-entries identified in a first ACL are contained in entries in a second ACL. In fact, an ACL in *Caronni* contains only entries of **target** hosts (i.e., other hosts other than the host that maintains the ACL). By definition, two ACLs in two different hosts will be different.

Caronni is devoid of any mention of identifying sub-entries in the first ACL, wherein at least one of the sub-entries is derived from the results of subtracting a particular access control entry specified in the first access control list from another access control entry specified in the same first access control list. At most, the cited portion in *Caronni* only pertains to a single entry in an ACL of a host that tracks the encryption capability of the other host. Since the cited portion pertains only to a single entry in an ACL, the cited portion of *Caronni* clearly fails to disclose subtracting a particular access control entry specified in the first access control list from another access control entry specified in the same first access control list, much less identifying sub-entries that includes the results of subtracting two entries specified in an ACL, as claimed.

For at least the reasons set forth above, Claim 33 is not anticipated by *Caronni*.

Claim 37

Claim 37 recites similar features as those discussed above with respect to Claim 3. Consequently, it is respectfully submitted that Claim 37 is not anticipated by *Caronni* for at least the same reasons discussed above as to Claim 33.

Claims 10, 11, 34, 35 and 38-41

Each of Claims 10, 11, 34, 35 and 38-41 contains all the features of Claim 33 or 37 discussed above and are patentable for the same reasons discussed above with respect to Claim 33 or 37. Further, each of Claims 10, 11, 34, 35 and 38-41 features steps that individually render them patentable. For all the foregoing reasons, Applicants respectfully submit that each of Claims 10, 11, 34, 35 and 38-41 is not anticipated by *Caronni*.

B. Claims 14 and 42 Are Patentable Over *Carroni* In View Of *Brawn*.

To establish obviousness, all the claim limitations must be taught or suggested by the prior art. *See In re Royka*, 490 F.2d 981, 985 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). "[I]n proceedings before the PTO, claims in an application are to be given their broadest reasonable interpretation consistent with the specification." *In re Sneed*, 710 F.2d 1544, 1548 (Fed. Cir. 1983). Thus, in adjudging obviousness, the Examiner may not ignore terms of a claim, and the interpretation of the claim terms must be reasonable, consistent with the description.

Each of Claims 14 and 42 contains all the features of Claim 33 or 37 discussed above and is patentable for the same reasons discussed above with respect to Claim 33 or 37. *Brawn* fails to disclose the features of Claim 33 or 37 that are missing in *Caronni*. Therefore, any combination of *Brawn* with *Caronni* fails to disclose the complete subject matter recited in Claims 14 and 42. For all the foregoing reasons, Applicants respectfully submit that Claims 14 and 42 are allowable over the cited references.

C. Claims 15 and 43 Are Patentable Over *Carroni* In View Of *Mate*.

Each of Claims 15 and 43 contains all the features of Claim 33 or 37 discussed above and is patentable for the same reasons discussed above with respect to Claim 33 or 37. *Mate* fails to disclose the features of Claim 33 or 37 that are missing in *Caronni*. Therefore, any combination of *Mate* with *Caronni* fails to disclose the complete subject matter recited in Claims 15 and 43. For all the foregoing reasons, Applicants respectfully submit that Claims 15 and 43 are allowable over the cited references.

D. Claims 16 and 44 Are Patentable over *Carroni* in view of *Banginwar*.

Each of Claims 16 and 44 contains all the features of Claim 33 or 37 discussed above and are patentable for the same reasons discussed above with respect to Claim 33 or 37. *Banginwar* fails to disclose the features of Claim 33 or 37 that are missing in *Caronni*. Therefore, any combination of *Banginwar* with *Caronni* fails to disclose the complete subject matter recited in

Claims 16 and 44. For all the foregoing reasons, Applicants respectfully submit that Claims 16 and 44 are allowable over the cited references.

VIII. CONCLUSION AND PRAYER FOR RELIEF

Based on the foregoing, it is respectfully submitted that the rejections of (a) Claims 10, 11, 33-35 and 37-41 under 35 U.S.C. § 102(b) as allegedly anticipated by *Caronni*; (b) Claims 14 and 42 under 35 U.S.C. § 103(a) as allegedly unpatentable over *Carroni* in view of *Brawn*; (c) Claims 15 and 43 under 35 U.S.C. § 103(a) as allegedly unpatentable over *Carroni* in view of *Mate*; and (d) Claims 16 and 44 under 35 U.S.C. § 103(a) as allegedly unpatentable over *Carroni* in view of *Banginwar*, lacks the requisite factual and legal bases. Appellants therefore respectfully request that the Honorable Board reverse the rejections of Claims 10, 11, 14-16, 33-35 and 37-44.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

/ZhichongGu#56543/
Zhichong Gu
Reg. No. 56,543

Date: May 29, 2009

2055 Gateway Place, Suite 550
San Jose, California 95110-1089
Tel: (408) 414-1236
Fax: (408) 414-1076

IX. CLAIMS APPENDIX

1-9. (Cancelled)

10. (Previously Presented) A method as recited in Claim 33, wherein identifying one or more first sub-entries in the first access control list comprises:

identifying a dimensional range and a policy action for each entry in the first access control list;

identifying all overlapping dimensional ranges in the first access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the first access control list overlap;

identifying all non-overlapping dimensional ranges in the first access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the first access control list that do not overlap dimensional ranges of other entries in the first access control list;

identifying a policy action for each identified overlapping dimensional range in the first access control list; and

identifying a policy action for each identified non-overlapping dimensional range of the first access control list.

11. (Previously Presented) A method as recited in Claim 35, wherein identifying second sub-entries in the second access control list comprises:

identifying a dimensional range and a policy action for each entry in the second access control list;

identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap;

identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list;

identifying a policy action for each identified overlapping dimensional range of the second access control list; and

identifying a policy action for each identified non-overlapping dimensional range of the

second access control list.

12-13. (Canceled)

14. (Previously Presented) A method as recited in Claim 10, wherein identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list.

15. (Previously Presented) A method as recited in Claim 10, wherein identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list.

16. (Previously Presented) A method as recited in Claim 10, wherein identifying a dimensional range and a policy action for each entry in the first access control list includes identifying a communication protocol for communication packets specified by each of the entries in the first access control list.

17-32. (Cancelled)

33. (Previously Presented) A method of comparing access control lists to configure a security policy on a network, the method comprising the computer-implemented steps of:

subtracting a particular access control entry from another access control entry, wherein both the particular access control entry and said another control entry are two access control entries of multiple first access control entries and wherein the first access control entries, including the particular access control entry and said another access control entry, are all of access control entries as specified in a first access control list;

identifying one or more first sub-entries in the first access control list, wherein the one or more first sub-entries include each of overlapping sections and non-overlapping sections of all of the first access control entries and wherein at least one of the one or more first sub-entries is derived from results of subtracting the particular access control entry from said another access control entry; and

programmatically determining whether the first access control list is functionally

equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is contained by one or more entries of multiple second access control entries in the second access control list.

34. (Previously Presented) A method as recited in Claim 33, further comprising determining that the first access control list is functionally equivalent to the second access control list in response to a determination that each of the first sub-entries is contained by one or more entries of the second access control list.

35. (Previously Presented) A method as recited in Claim 33, further comprising:
identifying second sub-entries in the second access control list, wherein the second sub-entries identified from the second access control list comprise (i) disjoint entries of the second entries or (ii) overlapping sections identified from the second entries or (iii) non-overlapping sections identified from the second entries; and
wherein determining whether each of the first sub-entry in the first access control list is contained by one or more entries of the second access control list includes determining whether the each of the first sub-entries in the first access control list is contained by one or more of the second sub-entries identified from the second control list.

36. (Canceled)

37. (Previously Presented) A policy server communicatively coupled to security devices in a network to configure a security policy on a network, the policy server comprising:
a processor;
a network interface that communicatively couples the processor to the network to receive flows of packets therefrom;
a memory; and
sequences of instructions in the memory which, when executed by the processor, cause the processor to carry out the steps of:
subtracting a particular access control entry from another access control entry, wherein both the particular access control entry and said another control entry are two access control entries of multiple first access control entries and wherein the first access control entries, including the particular access control entry and said

another access control entry, are all of access control entries as specified in a first access control list;

identifying one or more first sub-entries in the first access control list, wherein the one or more first sub-entries include each of overlapping sections and non-overlapping sections of all of the first access control entries and wherein at least one of the one or more first sub-entries is derived from results of subtracting the particular access control entry from said another access control entry; and

programmatically determining whether the first access control list is functionally equivalent to a second access control list by determining whether each of the first sub-entries in the first access control list is contained by one or more entries of multiple second access control entries in the second access control list.

38. (Previously Presented) A policy server as recited in Claim 37, wherein said sequence of instructions further comprising instructions for performing determining that the first access control list is functionally equivalent to the second access control list in response to a determination that each of the first sub-entries is contained by one or more entries of the second access control list.

39. (Previously Presented) A policy server as recited in Claim 37,

wherein said sequence of instructions further comprising instructions for performing identifying second sub-entries in the second access control list, wherein the second sub-entries identified from the second access control list comprise (i) disjoint entries of the second entries or (ii) overlapping sections identified from the second entries or (iii) non-overlapping sections identified from the second entries; and

wherein said instructions for performing determining whether each of the first sub-entry in the first access control list is contained by one or more entries of the second access control list include instructions for performing determining whether the each of the first sub-entries in the first access control list is contained by one or more of the second sub-entries identified from the second control list.

40. (Previously Presented) A policy server as recited in Claim 37, wherein said instructions for performing identifying one or more first sub-entries in the first access control list comprise:

instructions for performing identifying a dimensional range and a policy action for each entry in the second access control list;

instructions for performing identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap;

instructions for performing identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list;

instructions for performing identifying a policy action for each identified overlapping dimensional range in the second access control list; and

instructions for performing identifying a policy action for each identified non-overlapping dimensional range of the second access control list.

41. (Previously Presented) A policy server as recited in Claim 39, wherein said instructions for performing identifying second sub-entries in the second access control list comprise:

instructions for performing identifying a dimensional range and a policy action for each entry in the second access control list;

instructions for performing identifying all overlapping dimensional ranges in the second access control list, each overlapping dimensional range corresponding to where the dimensional ranges of entries in the second access control list overlap;

instructions for performing identifying all non-overlapping dimensional ranges in the second access control list, each of the non-overlapping dimensional ranges corresponding to dimensional ranges of entries in the second access control list that do not overlap dimensional ranges of other entries in the second access control list;

instructions for performing identifying a policy action for each identified overlapping dimensional range of the second access control list; and

instructions for performing identifying a policy action for each identified non-overlapping dimensional range of the second access control list.

42. (Previously Presented) A policy server as recited in Claim 40, wherein said instructions

for performing identifying a dimensional range and a policy action for each entry in the first access control list include instructions for performing identifying a source address range and a destination address range for communication packets specified by each of the entries in the first access control list.

43. (Previously Presented) A policy server as recited in Claim 40, wherein said instructions for performing identifying a dimensional range and a policy action for each entry in the first access control list include instructions for performing identifying a source port range and a destination port range for communication packets specified by each of the entries in the first access control list.

44. (Previously Presented) A policy server as recited in Claim 40, wherein said instructions for performing identifying a dimensional range and a policy action for each entry in the first access control list include instructions for performing identifying a communication protocol for communication packets specified by each of the entries in the first access control list.

45-48. (Canceled)

X. EVIDENCE APPENDIX

None

XI. RELATED PROCEEDINGS INDEX

None